Department of Defense

DIRECTIVE

NUMBER 4630.5

January 11, 2002

ASD(C3I)

SUBJECT: Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

References: (a) DoD Directive 4630.5, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," November 12, 1992 (hereby canceled)
(b) Division E of the Clinger-Cohen Act of 1996 (Chapter 25 of title 40, United States Code), as amended
(c) Sections 2223 and 2224 of title 10, United States Code, as amended
(d) Section 133 of title 10, United States Code
(e) through (g), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policy and responsibilities for interoperability and supportability of Information Technology (IT), including National Security Systems (NSS), to reflect DoD Chief Information Officer's (DoD CIO's) responsibilities contained in references (b) and (c).

1.2. Directs the use of a mission-related, outcome-based approach that considers both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership, personnel, or facilities) aspects to ensure interoperability and supportability of IT and NSS throughout the Department of Defense. This approach ensures that information is available to the Department of Defense in an assured, timely, useable, understandable, and cost-effective manner.

2. APPLICABILITY AND SCOPE

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies (see paragraph E2.1.2., below) the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively as "the DoD Components").

2.2. All IT, including NSS, acquired, procured (systems or services), or operated by any Component of the Department of Defense, to include:

2.2.1. All IT and NSS defense acquisition programs, defense technology IT and NSS projects, and IT and NSS pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations, Advanced Technology Demonstrations, and Joint Warrior Interoperability Demonstration Gold Nuggets when selected for acquisition or procurement), Joint Experimentation, and Joint Tests and Evaluations; non-5000 Series IT and NSS acquisitions or procurements (e.g., the Commander in Chief (CINC) Command and Control Initiative Program, CINC Initiatives Fund, CINC Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, and Tactical Exploitation of National Capabilities Programs); and post-acquisition (fielded) IT and NSS systems.

2.2.2. All inter- and intra-DoD Component IT and NSS that exchange and use information to enable units or forces to operate effectively in joint, combined, coalition, and interagency operations and simulations.

2.2.3. All IT and NSS acquired, procured, or operated by DoD intelligence agencies, DoD Component intelligence elements, and other DoD intelligence activities engaged in direct support of DoD missions. This Directive recognizes that special measures may be required for protection/handling of foreign intelligence or counterintelligence information, or other need to know information. Accordingly, implementation of this Directive must be tailored to comply with separate and coordinated Director of Central Intelligence (DCI) Directives and Intelligence Community policies.

2.2.4. All DoD IT and NSS external information exchange interfaces with other U.S. Government Departments and Agencies, combined and coalition partners, and multinational alliances (e.g., North Atlantic Treaty Organization).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. IT and NSS interoperability and supportability are essential to joint, combined and coalition forces working together seamlessly to enhance operational effectiveness. Attaining IT and NSS interoperability and supportability is a continuous process, addressed as a balance of materiel and non-materiel solutions that is achieved and sustained throughout a system's life. Achieving and sustaining interoperability and supportability is a DoD enterprise-wide responsibility that must be woven into the thread of organizational roles, responsibilities, processes, and resources.

4.2. The Department of Defense shall achieve and maintain information superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining and leveraging interoperable and supportable IT and NSS. IT and NSS interoperability and supportability shall be attained through mission-related, outcome-based processes. Interoperability and supportability requirements shall be balanced with the need for Information Assurance. Joint, combined, coalition, and interagency missions must be supported through interoperable IT and NSS in global operations across the peace-conflict spectrum.

4.3. For the purposes of interoperability and supportability, IT and NSS used by U.S. Forces shall be developed with the capability to meet essential operational needs, and where required, shall interoperate with existing and planned, functionally related, systems and equipment of joint, combined and coalition forces; and with other U.S. Government Departments and Agencies, as appropriate.

4.4. IT and NSS interoperability and supportability requirements shall be characterized through operational mission area integrated architectures, operational concepts and Capstone Requirements Documents derived from Joint Mission Areas (JMAs) and business/administrative mission areas. The Joint Operational Architecture (JOA), the Joint Systems Architecture (JSA), and the Joint Technical Architecture (JTA) shall serve as the foundation for development of mission area integrated architectures. Mission area integrated architectures shall relate IT and NSS interoperability and supportability requirements in a Family-of-Systems/System-of-Systems (FoS/SoS) context. IT and NSS FoS/SoS Information Exchange Requirements (IERs) and associated interoperability Key Performance Parameters

(KPPs) shall be derived from the operational view of the mission area integrated architecture.

4.5. IT and NSS interoperability and supportability needs shall be identified through the requirements definition and validation process, in conjunction with the acquisition process, and shall be updated as necessary throughout the system's life. IT and NSS interoperability and supportability requirements shall be specified to a level of detail that allows verification of interoperability throughout a system's life. For IT and NSS defense acquisition and procurement programs, an interoperability KPP shall be defined during the requirements definition and validation process. The defined interoperability KPP shall be developed in such a way that it can be reliably measured tested and evaluated. If an evolutionary acquisition strategy is employed, IT and NSS interoperability and supportability requirements shall evolve consistent with the evolutionary acquisition approach.

4.6. IT and NSS interoperability and supportability shall be managed, evaluated, and reported over the life of the system using an existing program support or management plan format. The support or management plan shall contain detailed and time-phased information for identifying dependencies and interface requirements, consistent with mission area integrated architectures, focusing attention on interoperability, supportability, and sufficiency concerns. For IT and NSS defense acquisition programs and procurements, system dependencies and interface requirements shall be described in sufficient detail to assist in acquisition and procurement decisions, and to provide test planners the information necessary to ensure that the system test program is sufficient to permit an accurate assessment of the systems' KPP capabilities and limitations. For non-acquisition designated IT and NSS programs, the program support or management plan shall contain sufficient detail (commensurate with the size of the program/effort) to permit an evaluation of the associated interoperability and supportability requirements.

4.7. IT and NSS shall be tested early and with sufficient frequency throughout a system's life or upon changes affecting interoperability or supportability to assess, evaluate, and certify its overall level of interoperability and supportability. This certification will be cost effective and shall be successfully completed prior to fielding of new IT and NSS or prior to fielding a new capability or upgrade to existing IT and NSS.

4.8. The process for improving IT and NSS interoperability and supportability shall provide solution sets focused on mission-based outcomes that address both materiel and non-materiel aspects. Once IT and NSS interoperability solution sets are validated, appropriate resources shall be recommended to implement identified remedies. As part of this process, the operational community shall identify, prioritize, and synchronize non-materiel solutions with materiel solutions to resolve interoperability and supportability issues.

4.9. IT and NSS interoperability and supportability oversight and direction shall be jointly provided by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); the Under Secretary of Defense (Comptroller) (USD(C))/DoD Chief Financial Officer (DoD CFO); the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)), ASD(C3I) as the DoD CIO; the Director, Operational Test and Evaluation (DOT&E); the Chairman of the Joint Chiefs of Staff; and the Commander in Chief, U.S. Joint Forces Command (USCINCJFCOM), as appropriate.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, shall:

5.1.1. Ensure, with the USD(AT&L), USD(C)/DoD CFO, the Chairman of the Joint Chiefs of Staff, DOT&E, and U.S. Joint Forces Command, that IT and NSS interoperability and supportability issues are addressed during the acquisition or procurement process. Ensure interoperability and supportability requirements, particularly cross-system and cross-Service, are identified and recommended for programming and budgeting.

5.1.2. Advise the Deputy Secretary of Defense, in coordination with the affected DoD Components, regarding alternative solutions and funding needs to meet interoperability and supportability shortfalls.

5.1.3. Ensure that the Director, Defense Information Systems Agency (DISA), establishes and conducts an IT and NSS interoperability assessment, test, evaluation, and certification program in collaboration with the DoD Components. Results from DISA interoperability assessments, tests, evaluations, and certifications shall conform to applicable security classification guidance to avoid potential compromise of information that may reveal component and/or system susceptibilities and vulnerabilities.

5.1.4. As the Chairman of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), consider requests for release of Information Security (INFOSEC) products or associated INFOSEC information to a foreign government or an international organization when required to achieve combined or coalition interoperability.

5.1.5. Ensure that the Director, National Security Agency, prescribes information assurance policy and procedures for safeguarding IT and NSS capabilities.

5.2. The <u>Assistant Secretary of Defense for Command, Control, Communications, and Intelligence</u>, as the <u>Department of Defense Chief Information Officer</u>, shall:

5.2.1. Maintain this Directive, with the other DoD Components, to codify the policies and responsibilities necessary to ensure interoperability and supportability of IT and NSS throughout the Department of Defense.

5.2.2. Provide policy, guidance, and oversight, with the DoD Components, to ensure that IT and NSS are interoperable and supportable with other relevant IT and NSS internal and external to the Department of Defense.

5.2.3. Ensure the development, implementation, and maintenance of a sound and integrated Information Technology Architecture (ITA) for all DoD IT and NSS, as required by reference (b). Ensure, with the USD(AT&L), the Chairman of the Joint Chiefs of Staff, and U.S. Joint Forces Command that FoS/SoS IT and NSS mission area integrated architectures are defined, developed, integrated, coordinated, validated, synchronized, and implemented.

5.2.4. Establish responsibilities and procedures, with the USD(AT&L), DOT&E, the DoD Components, the Chairman of the Joint Chiefs of Staff, and U.S. Joint Forces Command, to ensure early assessment, verification, evaluation and certification of IT and NSS interoperability and supportability throughout a system's life. The DoD CIO, with the DoD Components, shall also ensure user-defined, mission-related, outcome-based performance measures are established for use in assessment and verification of IT and NSS interoperability and supportability.

5.2.5. Develop a process, with the DoD Components, to annually evaluate Department of Defense IT and NSS interoperability and supportability status. Findings will be reported to the Deputy Secretary of Defense in sufficient time to support the Department's budgeting decisions.

5.2.6. Define, organize, and approve, with the USD(AT&L), the Chairman of the Joint Chiefs of Staff, and the DoD Components, Universal Reference Resources (URRs) for developing mission area integrated architectures throughout the Department of Defense.

5.2.7. Maintain a consolidated inventory, and identify associated interfaces, for DoD Mission Critical Information Systems (MCIS) and Mission Essential Information Systems (MEIS).

5.2.8. Prescribe, with the DoD Components, approved IT and NSS standards that apply throughout the Department of Defense. For non-Acquisition Category (ACAT) and procurement matters, the prescription of IT and NSS standards will consider tradeoffs among operational effectiveness, operational suitability, and IT and NSS interoperability and supportability.

5.2.9. Review, assess, and evaluate IT and NSS acquisitions and procurements, and, with the DoD Components, propose recommendations to the Secretary of Defense for the elimination of unnecessary duplication of IT and NSS within and among the DoD Components.

5.2.10. Provide the Deputy Secretary of Defense, with USD(AT&L), USD(C)/DoD CFO, the Chairman of the Joint Chiefs of Staff, the DoD Components, and U.S. Joint Forces Command, material and non-material recommendations for resolving critical IT and NSS interoperability and supportability issues. These recommendations shall be prioritized and phased for acquisition (or procurement) and implementation.

5.3. The Under Secretary of Defense for Acquisition, Technology and Logistics shall:

5.3.1. As the Department of Defense Acquisition Executive (reference (d)), ensure the policies outlined in section 4., above, are incorporated into the 5000 series of DoD issuances (references (e), (f), and (g)) and addressed during systems acquisition, as appropriate.

5.3.2. For all acquisition matters, with the DoD CIO, the Chairman of the Joint Chiefs of Staff, and U.S. Joint Forces Command, approve tradeoffs among operational effectiveness, operational suitability, and IT and NSS interoperability and supportability.

5.3.3. Define policy and procedures, with the DoD CIO and the DOT&E, for a management process, using a support or management plan for ensuring IT and NSS interoperability and supportability over a system's life.

5.3.4. Establish responsibilities and procedures, with the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and U.S. Joint Forces Command, for assessing and verifying interoperability KPPs throughout a system's life. Ensure mission-related, outcome-based performance measures are established for assessing and verifying IT and NSS interoperability and supportability.

5.3.5. Ensure, with DoD CIO and the Chairman of the Joint Chiefs of Staff, that approved architectural framework concepts and products are incorporated into acquisition guidance and policy.

5.3.6. Identify, coordinate, and integrate DoD system architecture views into an overall DoD-wide JSA.

5.4. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall:

5.4.1. Ensure, with affected DoD Components, IT and NSS interoperability and supportability funding issues resulting from the requirements of this Directive are addressed in the budgetary process.

5.4.2. Provide the Deputy Secretary of Defense, with USD(AT&L), DoD CIO, the Chairman of the Joint Chiefs of Staff, the other DoD Components, and U.S. Joint Forces Command, budget recommendations for addressing critical IT and NSS interoperability and supportability issues.

5.5. The Director of Operational Test and Evaluation shall:

5.5.1. Coordinate with the Chairman of the Joint Chiefs of Staff and U.S. Joint Forces Command, to ensure interoperability KPPs specified in requirements documents are measurable and contribute to the evaluation of a system's operational effectiveness and suitability.

5.5.2. Develop policy, processes, practices and test infrastructure, with USD(AT&L) and the DoD CIO, to ensure IT and NSS interoperability and supportability are evaluated as a measure of operational effectiveness throughout all test programs. Ensure interoperability test requirements are identified in test and evaluation master plans and operational test plans. Emphasize evaluation of IT and NSS interoperability and supportability, in a FoS/SoS environment, as early as possible during a system's development.

5.5.3. Provide an assessment of interoperability and related supportability at acquisition milestones. Report results of these interoperability and supportability assessments as part of the DOT&E Annual Report to Congress.

5.5.4. Assist the DoD Components with test planning and assessment of FoS/SoS IT and NSS interoperability and supportability.

5.6. The Heads of the DoD Components shall:

5.6.1. Ensure the requirements of this Directive are implemented, including the establishment of procedures for: the development, coordination, review, and verification of IT and NSS interoperability and supportability requirements; IT and NSS acquisition or procurement; and testing within respective functional areas.

5.6.2. Ensure interoperability and supportability capabilities are designed, developed, tested, evaluated, and incorporated into all DoD Component IT and NSS. When necessary, recommend tradeoffs among operational effectiveness, operational suitability, and IT and NSS interoperabilty and supportability to USD(AT&L), the DoD CIO, the Chairman of the Joint Chiefs of Staff, and U.S. Joint Forces Command.

5.6.3. Ensure IT and NSS interoperability and supportability requirements are identified and accommodated in respective DoD Components' budgets. When necessary, propose alternative programmatic, technical and funding solutions to meet IT and NSS interoperability and supportability shortfalls to USD(AT&L), the DoD CIO, the Chairman of the Joint Chiefs of Staff, and U.S. Joint Forces Command.

5.6.4. Implement procedures to ensure the use of DoD JTA, Common Operating Environment (COE) technical guidance, and COE technology for programs under the DoD Components' cognizance.

5.6.5. Ensure test and evaluation plans are prepared for all IT and NSS acquisitions and procurements.

5.6.6. Develop procedures for all IT and NSS acquisitions and procurements to document, manage, evaluate, and report on IT and NSS interoperability throughout a system's life using a program support or management plan.

5.6.7. Provide results of all developmental and operational joint interoperability assessments, tests and evaluations to USD(AT&L), the DoD CIO, DOT&E, the Chairman of the Joint Chiefs of Staff, and U.S. Joint Forces Command.

5.7. The <u>Chairman of the Joint Chiefs of Staff</u> shall:

5.7.1. Establish policy and procedures, with U.S. Joint Forces Command and other DoD Components, for the development, coordination, review, and approval of IT and NSS interoperability and supportability requirements.

5.7.2. Develop, approve, and direct the use of the JMA-based JOA to facilitate the identification of IT and NSS interoperability and supportability requirements within a FoS/SoS context.

5.7.3. Develop, approve, and issue joint-doctrinal concepts and associated operational procedures to achieve interoperability and supportability of IT and NSS capabilities employed by U.S. Military Forces and, where required, with: joint, combined, and coalition forces; and with other U.S. Government Departments and Agencies.

5.7.4. Review and certify IT and NSS IERs, resultant interoperability KPP, and other requirements as derived from mission area integrated architectures.

5.7.5. Establish, with USD(AT&L), the DoD CIO, DOT&E, and U.S. Joint Forces Command, procedures for verification of interoperability for fielded IT and NSS throughout a system's life.

5.7.6. Establish a process to ensure insights are gained from Joint Exercises on IT and NSS interoperability and supportability and coordinated with the DoD CIO and USD(AT&L).

5.8. The <u>Commander in Chief, U.S. Joint Forces Command</u> shall:

5.8.1. Serve as the Chief Advocate for Interoperability by assessing IT and NSS interoperability requirements from the warfighter's perspective in accordance with Chairman of the Joint Chiefs of Staff responsibilities to review and confirm IERs and interoperability KPPs ensuring new systems and capabilities address interoperability and supportability from inception throughout a system's life.

5.8.2. Solicit from the CINCs joint, combined, and coalition IT and NSS interoperability and supportability issues.

5.8.3. Identify, consolidate, and prioritize IT and NSS interoperability and supportability issues affecting fielded systems in coordination with the CINCs.

5.8.4. Provide operationally prioritized and programmatically synchronized materiel and non-materiel recommendations for resolving IT and NSS interoperability issues to the Chairman of the Joint Chiefs of Staff. Coordinate recommendations with USD(AT&L), USD(C)/DoD CFO, the DoD CIO, and the Chairman of the Joint Chiefs of Staff.

6. <u>EFFECTIVE DATE</u>

This Directive is effective immediately.

Paul Wolfowitz

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
E1. References, continued
E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Directive 5000.1, "The Defense Acquisition System," October 23, 2000

(f) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," October 23, 2000

(g) DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," June 10, 2001[1]

[1] Copies may be obtained via Internet at http://www.acq.osd.mil/ap/50002-R_Final_June_10201_with_signatures.doc

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Architectures. The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

E2.1.2. Defense Agencies. All agencies and offices of the Department of Defense including the Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Imagery and Mapping Agency, National Reconnaissance Office, and National Security Agency.

E2.1.3. Family-of-Systems (FoS). A set or arrangement of independent systems that can be interconnected or related in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation or mission.

E2.1.4. Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.5. Information Exchange Requirements (IERs). The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as, why the information is necessary and how that information shall be used.

E2.1.6. Information Superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

E2.1.7. Information Technology (IT). Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT"also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT"does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT"includes National Security Systems (NSS).

E2.1.8. Information Technology Architecture (ITA). An integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the Agency's strategic goals and information resources management goals.

E2.1.9. Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, systems view, and technical view) that facilitates integration and promotes interoperability across Family-of-Systems/System-of-Systems and compatibility among related mission area architectures.

E2.1.9.1. The operational architecture view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a warfighting function.

E2.1.9.2. The systems architecture view is a description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions.

E2.1.9.3. The technical architecture view is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

E2.1.10. Interoperability. Interoperability is the ability of systems, units or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment.

E2.1.11. Joint Mission Areas (JMAs). JMAs represent a functional group of joint tasks and activities that share a common purpose, and facilitate joint-force operation and interoperability. JMAs provide a logical way to organize the Joint Operational

Architecture. JMAs provide the context for defining FoS/SoS relationships sharing a common mission area.

E2.1.12. Joint Operational Architecture (JOA). Description of tasks and activities, operational elements, and information flows required to accomplish or support military operations; defines types of information exchanged, frequency of exchange, which tasks and activities are supported by information exchanges, and nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

E2.1.13. Joint Systems Architecture (JSA). The identification and description of all DoD systems and their interconnections necessary to accomplish the tasks and activities described in the Joint Operational Architecture.

E2.1.14. Joint Technical Architecture (JTA). The JTA provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems, and its adoption is mandated for the management, development, and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense.

E2.1.15. Key Performance Parameters (KPPs). Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet a KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a Capstone Requirements Document KPP threshold can be the cause for the FoS/SoS concept to be reassessed or the contributions of the individual systems to be reassessed.

E2.1.16. Materiel Solution. Correction of a deficiency, satisfaction of a need, or incorporation of new technology that results in the development, acquisition, procurement or fielding of a new item (including ships, tanks, self-propelled weapons, aircraft, etc., and related software, spares, repair parts and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without disruption as to its application for administrative or combat purposes.

E2.1.17. Mission Area Integrated Architectures. Mission area integrated architectures are the common foundation for mission area focused, outcome-based IT and NSS interoperability and supportability processes. Mission area integrated architectures (consisting of operational, systems, and technical views) are derived from JMAs (i.e., subordinate/supporting missions to the JMAs) and/or business/administrative mission areas. Mission area integrated architectures can cover organizational entities (e.g., Joint Task Force, Navy Battle Group or Army Brigade). The Joint Operational Architecture (JOA), the Joint Systems Architecture (JSA) and the Joint Technical Architecture (JTA) serve as the basis for developing mission area integrated architectures.

E2.1.18. Mission Critical Information Systems (MCIS). A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act (reference (b)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical should be made by a Component Head, a CINC or their designee.) A Mission Critical Information Technology System has the same meaning as a Mission Critical Information System.

E2.1.19. Mission Essential Information Systems (MEIS). A system that meets the definition of "information system" in the Clinger-Cohen Act (reference (b)), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission essential should be made by a Component Head, a CINC or their designee.)

E2.1.20. Non-Materiel Solution. Changes in doctrine, organization, training, leadership, personnel or facilities that satisfy identified mission needs.

E2.1.21. National Security System (NSS). Any telecommunications or information system operated by the United States Government, the function, operation, or use of which:

E2.1.21.1. Involves intelligence activities.

E2.1.21.2. Involves cryptologic activities related to national security.

E2.1.21.3. Involves command and control of military forces.

E2.1.21.4. Involves equipment that is an integral part of a weapon or weapons system.

E2.1.21.5. Is critical to the direct fulfillment of military or intelligence missions. This does not include automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance logistics and personnel management applications).

E2.1.22. Operational Concept. An end-to-end stream of activities that defines how force elements, systems, organizations, and tactics combine to accomplish a military task.

E2.1.23. Outcome-Based Interoperability. An interoperability process that:

E2.1.23.1. Includes experts from the operational community to identify, consolidate and prioritize interoperability deficiencies; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities.

E2.1.23.2. Characterizes IT and NSS interoperability requirements in a family-of-systems or system-of-systems mission area context and relates IT and NSS through integrated architectures derived from the Joint Operational Architecture and associated Joint Mission Areas.

E2.1.23.3. Precisely defines operational user requirements to include interoperability as a Key Performance Parameter.

E2.1.23.4. Incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership, personnel, or facilities) solutions.

E2.1.23.5. Verifies solution sets in formal tests or operational exercises.

E2.1.23.6. Continuously evaluates interoperability Key Performance Parameters and verifies overall IT and NSS interoperability throughout a system's life.

E2.1.24. Supportability. The ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain design, development, testing, training, or operations of the IT or NSS to its required capability.

E2.1.25. System-of-Systems (SoS). A set or arrangement of systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

E2.1.26. Universal Reference Resources (URRs). Reference models and information standards, which serve as sources for guidelines and attributes that must be consulted while building integrated architecture products. The following are the currently listed URRs: DoD Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture Framework; C4ISR Core Architecture Data Model; Defense Data Dictionary, Levels of Information Systems Interoperability; Universal Joint Task List; Joint Operational Architecture; Technical Reference Model; Defense Information Infrastructure Common Operating Environment; Shared Data Environment; and the DoD Joint Technical Architecture.